

Abstract of the Disclosure

Let us consider a message M an element (m_1, m_2, \dots, m_k) in a Galois field $GF(2^k)$, and multiply it by a product of polynomials $\beta_1(\alpha) \cdot \beta_2(\alpha) \cdot \dots \cdot \beta_t(\alpha)$ into $M(\alpha)$.

$$M(\alpha) = M \beta_1(\alpha) \cdot M \beta_2(\alpha) \cdot \dots \cdot M \beta_t(\alpha)$$

Combine a noise vector $r(\alpha)$ of $n - k$ to $M(\alpha)$ in series so that the data is expanded into degree n . Next, they are transformed into Γ by permutation. Γ is multiplied by an element γ^x in the Galois field $GF(2^n)$ into cyphertext $C(M)$, where γ is a primitive root of the multiplicative group of the Galois field $GF(2^n)$.

Practically, when the message M is substituted for X in a public key $C(X)$, the cyphertext $C(M)$ is obtained. The cyphertext $C(M)$ is multiplied by γ^{-x} , is applied to an inverse permutation, and the noise vector $r(\alpha)$ is separated. Then, the inverse element of the product of $\beta_1(\alpha) \cdot \beta_2(\alpha) \cdot \dots \cdot \beta_t(\alpha)$ is multiplied and is raised to an adequate index. Then the decrypted message is obtained.